AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (original): A digital camera, comprising:

an image pickup portion which converts light from an object to be photographed, into image data;

a producing device which produces characteristic data from the image data;

a secret key-recording portion which records a secret key to be used for encrypting data so that encrypted data can be decrypted by a public key;

an encrypting device which encrypts the characteristic data with the secret key;

an embedding device which embeds encrypted characteristic data into the image data;

a recording medium which records the image data having the characteristic data embedded therein; and

a transmitting device which transmits the secret key from an external recording medium.

2. (original): A digital camera, comprising:

an image pickup portion which converts light from an object to be photographed, into image data;

a producing device which produces characteristic data from the image data;

a secret key-recording portion which records a secret key to be used for encrypting data so that encrypted data can be decrypted by a public key;

an encrypting device which encrypts the characteristic data with the secret key;

an embedding device which embeds encrypted characteristic data into the image data; and

a recording medium which records the image data having the characteristic data embedded therein,

wherein the secret key is recorded in the secret key-recording portion in a form of a hidden attribute.

3. (original): A method of adding to a digital camera a function of converting light from an object to be photographed, into image data, the method comprising the steps of:

selecting, from among a plurality of data volumes, the volume of data pertaining to a secret key for encrypting data so that encrypted data can be decrypted by a public key;

recording the secret key into a secret key-recording portion of the digital camera from an external recording medium; and

loading an encryption program into the digital camera through use of the secret key.

4. (original): The method of claim 3, wherein the secret key is recorded in a form of a hidden attribute.

5. (original): An image falsification detection system using a digital camera which comprises an image pickup portion which converts light from an object to be photographed, into image data, a first producing device which produces first characteristic data from the image data, a secret key-recording portion which records a secret key to be used for encrypting data so that encrypted data can be decrypted by a public key, an encrypting device which encrypts the first characteristic data with the secret key, an embedding device which embeds encrypted first characteristic data into the image data, and a recording medium which records the image data having the first characteristic data embedded therein, the image falsification detection system comprising:

an inputting device which inputs the image data;

a removing device which removes the encrypted first characteristic data from the image data;

a decrypting device which decrypts the encrypted first characteristic data;

a second producing device which produces second characteristic data from the image data from which the encrypted first characteristic data have been removed; and

a comparing device which compares the decrypted first characteristic data with the second characteristic data.

6. (original): The image falsification detection system of claim 5, further comprising a recording device which records a plurality of public keys corresponding to a plurality of secret keys.

7. (original): The image falsification detection system of claim 5, further comprising a transmitting device which transmits the secret key from an external recording medium.

8. (original): The image falsification detection system of claim 5, wherein the secret key is recorded in the secret key-recording portion in a form of a hidden attribute.

9. (new): The method of claim 3, wherein the secret key is selected in order to achieve a desired level of encryption sophistication.